UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/822,226	04/08/2004	Sumeet Singh	15670-075001/ SD2004-151	1313

20985 7590 05/23/2008

FISH & RICHARDSON, PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
OKORONKWO, CHINWENDU C	
ART UNIT	PAPER NUMBER
2136	
MAIL DATE	DELIVERY MODE
05/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/822,226	SINGH ET AL.	
	Examiner	Art Unit	
	CHINWENDU C. OKORONKWO	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,11-15,20,21,33-35,69,71,75,79,88 and 89* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,11-15,20,21,33-35,69,71,75,79,88 and 89* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/28/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. In response to communications filed on 01/28/2008, the Examiner acknowledges the amendments made to the claims and have both considered and applied them to the claims.

In response to communications filed on 01/28/2008, claims 1 – 35, 69 – 79, 88 and 89 are pending.

Response to Remarks/Arguments

1.1 Applicant's arguments, pages 18 – 24, with respect to the rejection of claims 1 – 35, 69 – 79, 88 and 89 have been fully considered but they are not persuasive.

1.2 In response to Applicant argument that the Cox reference does not teach or suggest data reduction or packetization, Examiner respectfully disagrees and in addition to the previous citation and obvious reasoning as explained in previous office action, the Cox et al. is silent in disclosing the carrying out a data reduction on said portion, however it would have been obvious to one of ordinary skill in the art to modify the disclosed invention to reduce said data portions. This would be obvious to one of ordinary skill in the art because one of ordinary skill would know that the "data packets (col. 1 lines 60-67 of Cox)" – which by definition are ***reductions of the original data*** (hence the name "packet") – are better handled and analyzed in smaller portions. Therefore, motivation and benefit for this modification would be to allow for the received packet to be properly analyzed.

In response to the applicants argument that Cox focuses on blocking attacks on a network, not on the identification of common content to use in blocking attacks, Examiner respectfully disagrees and in addition to the previous citation and obvious reasoning as explained in previous office action submits that Cox recites in column 3 lines 36-39, "known patterns ... can be built using knowledge about various types of attacks" and as agreed by Applicant on page 22 of his arguments that it is matched against known patterns which in essentiality means common content is being matched. Therefore, as understood by the examiner, the Applicant is contradicting his own statement.

Applicant has not overcome the rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Claims 1-6, 11-15, 20-21, 33-35, 69, 71, 75, 79, 88 and 89 and rejected under 35 U.S.C. 102(e) as being disclosed by Cox et al. (US Patent No. 6,738,814 B1).

Regarding claim 1, Cox et al., discloses a method for automatically identifying common content to use in identifying an intrusive network attack comprising: obtaining a collection of data to be analyzed to identify the network attack; reducing said data items [[on]] in said collection to

reduce said data collection to a reduced data collection of reduced data items, wherein the reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item and analyzing a plurality of said reduced data items to detect common elements, said analyzing reviewing for common content indicative of a network attack (col. 1 lines 60-67 – "analyzing an incoming data packet from the public network. The incoming data packet is then matched against known forms of attack on the private network").

> The Examiner understands Cox et al. to disclose data reduction in the column 1 lines 60-67 recitation of "data packets" which, by definition, are ***reductions of the original data*** (hence the name "packet") and are better handled and analyzed in smaller portions. The Examiner therefore understands the data packet of Cox et al. to read upon and be the result of data reduction as claimed by the Applicant.

Regarding claim 2, Cox et al., discloses a method as in claim 1, wherein said analyzing comprises determining frequently occurring sections of message information (col. 1 lines 60-67 – "analyzing an incoming data packet from the public network. The incoming data packet is then matched against known forms of attack on the private network.").

Regarding claim 3, Cox et al., discloses a method as in claim 1, wherein said analyzing comprises determining that increasing number of sources and destinations that are sending

and/or receiving data (col. 1 line 67 and col. 2 lines 1-7).

Regarding claim 4, Cox et al., discloses a method as in claim 1, further comprising analyzing for the presence of a specified type of code within said collection of data (col. 1 lines 60-67 – "analyzing an incoming data packet from the public network. The incoming data packet is then matched against known forms of attack on the private network.").

Regarding claim 5, Cox et al., discloses a method as in claim 2, further comprising, after said analyzing determines said frequently occurring sections of message information, carrying out an additional test on said frequently occurring sections of message information (col. 3 lines 34-45 – "based upon pattern matching … the routing device can identify the data packet and its source as malicious or non-malicious").

Regarding claim 6, Cox et al., discloses a method as in claim 5, wherein said carrying out the additional test comprises looking for an increasing number of at least one of sources and destinations of said frequently occurring sections of message information (col. 3 lines 54 – "routing device compares the IP address of the packet against known internal IP addresses of the associated private network … if the source IP address").

Regarding claim 11, Cox et al., discloses additional test comprising maintaining a first list of unassigned addresses, forming a second list of sources that have sent to addresses on said

first list and comparing a current source of a frequently occurring section to said second list (col. 3 lines 54-65).

Regarding claim 12, Cox et al., discloses a method as in claim 11, wherein said carrying out the addition al test comprises reducing addresses in said first list and said second list to reduced addresses, wherein the reduced addresses have a smaller size and a constant predetermined relation with the addresses and at least some of the addresses that differ are reduced to the same reduced to the same reduced address (col. 3 lines 54-65).

Regarding claim 13, Cox et al., discloses a method as in claim 5, wherein said carrying out the additional test comprises: first monitoring a first content sent to a destination; second monitoring a second content sent by said destination; and determining a correlation between said first content and said second content (col. 4 lines 1-14).

Regarding claim 14, Cox et al., discloses a method as in claim 13, wherein said first monitoring comprises monitoring multiple destinations, and said second monitoring comprises monitoring multiple destinations during a different time period than said first monitoring (col. 4 lines 15-26).

Regarding claim 15, Cox et al., discloses a method as in claim 14, wherein said first and second monitoring comprises reducing information about said destinations, and storing at least one table about said data reduced information (col. 4 lines 1-26).

Regarding claim 20, Cox et al., discloses method as in claim 1, further comprising forming a plurality of data items from each of a collection of network packets, each of said plurality of data items comprising a specified subset of the network packets (Rejected under the combined rationales as claim 1).

Regarding claim 21, Cox et al., discloses a method as in claim 1, further comprising forming a plurality of data items from each of a collection of network packets, each of said plurality of data items comprising a continuous portion of payload and information indicative of a port number indicating a service requested by the network packet (Rejected under the combined rationales as claims 11 and 20).

Regarding claim 33, Cox et al., discloses a method as in claim 1, further comprising, determining a list of first computers that are susceptible to a specified attack, and monitoring only messages directed to said first computers for said specified attack (Rejected under the same rationale as claim 1).

Regarding claim 34, Cox et al., discloses a method of claim 33 where said monitoring comprises checking for a message that attempts to exploit a known vulnerability to which a computer is vulnerable, as said specified attack (Rejected under the same rationale as claim 1).

Regarding claim 35, Cox et al., discloses a method as in claim 34, wherein said checking comprises checking for a field that is longer than a specified length (Rejected under the same rationale as claim 1).

Regarding claim 69, Cox et al., discloses a method for automatically identifying common content to use in identifying an intrusive network attack, comprising: monitoring network content on a network, and obtaining at least portions of the data on said network; data reducing said portions of the data using a data reduction function which reduces said portions of the data to reduced data portions in repeatable manner, such that each portion which has the same content is reduced to the same reduced data portion and at least some of the portions that differ are reduced to the same reduced data portion; analyzing said reduced data portions to find network content which repeats a specified number of times, and to establish said network content which repeats said specified number of times as frequent content; identifying address information of said frequent content, wherein the address information includes at least one of source information or destination information that characteristizes the respective of sources and/or destinations, of said frequent content, and determining if a number of sources and/or destinations of said frequent content is increasing; and identifying the frequent content as associated with the network attack, based on said identifying and determining (Rejected under the same rationale as claim 1).

Regarding claim 71, Cox et al., discloses a method as in claim 70, wherein said obtaining portions of the network data comprises: defining a window which samples a first portion of

network data at a first time in accordance with a position of the window, and sliding said window to a second position at a second time which samples a second portion of said network data wherein said second position has a specified offset from the first portion (Rejected under the same rational as claim 1).

Regarding claim 75, Cox et al., discloses a method as in claim 69, wherein said identifying comprises second data reducing said address information using a data reduction function, and maintaining a table of data reduced address information (Rejected under the same rationale as claim 1).

Regarding claim 79, Cox et al., discloses a method as in claim 69, further comprising monitoring for scanning of addresses (Rejected under the same rationale as claim 11).

Regarding claim 88. Cox et al. discloses a method for automatically identifying common content to use in identifying an intrusive network attack, comprising: obtaining a collection of data items to be analyzed to identify the network attack; reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, wherein the reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item; analyzing a plurality of said reduced data items to determine frequently occurring sections of message information indicative of a network attack; and carrying out an additional test on said

frequently occurring sections of message information, comprising maintaining a first list of unassigned addresses, wherein the unassigned addresses are maintained as reduced addresses that have a smaller size and a constant predetermined relation with the unassigned addresses and at least some of the unassigned addresses that differ are reduced to the same reduced address, forming a second list of source addresses that have sent to the unassigned addresses on said first list, wherein the source addresses are maintained as reduced addresses that have a smaller size and a constant predetermined relation with the source addresses and at least some of the source addresses that differ are reduced to the same reduced address, and comparing a current source of a frequently occurring section to said second list (Rejected under the same rationale as claim 1 and 12).

Regarding claim 89. Cox et al. discloses a method for automatically identifying common content to use in identifying an intrusive network attack, comprising: obtaining a collection of data items to be analyzed to identify the network attack, wherein said data items comprise a first subset of a network packet including payload and header; reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, wherein the reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item; analyzing a plurality of said reduced data items to detect common elements, said analyzing reviewing for common content indicative of a network attack; and obtaining a second subset of

the same network packet for subsequent analysis (Rejected under the same rationale as claim 1 and 12).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 7-9, 16-19, 22-32, 70-74 and 76-78 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cox et al. (US Patent No. 6,738,814 B1) and further in view of Townshend (US Patent No. 6,829,635 B1).

Regarding claim 7, Cox et al., is silent in disclosing a method as in claim 5, wherein said carrying out the additional test comprises looking for code or opcode (operation code) within the frequently occurring sections, however it would have been obvious for one of ordinary skill in the art to modify the invention disclosed by Cox into the claimed invention due to disclosure of the comparison between the "requested connection and one or more existing connections (col. 4 lines 29-31)." It would have been obvious because the connection requests are codes to various connection ports. Therefore to look for code or opcode within sections of data is an obvious reference to connection port codes, which Cox does disclose (col. 4 lines 15-39).

Regarding claim 8, Cox et al., is silent in disclosing a method wherein said reducing said data items comprises carrying out a hash function on said data items, however Towshend does disclose such hashing in column 6 lines 39-56. It would have been obvious to combine these two inventions and the motivation would be to improve the storage of the patterns disclosed by Cox in column 3 lines 36-39 which recites, "known patterns ... can be built using knowledge about various types of attacks. This knowledge can be recorded in the form of patterns that are then stored in a database or other storage device accessible by the routing device."

Regarding claim 9, Cox et al., does not explicitly disclose a method wherein said determining frequently occurring sections comprises using at least first, second and third data reduction techniques on each said data item, to obtain at least first, second and third reduced data items, counting said first, second and third reduced data items, and establishing said frequently occurring sections when all of said at least first second and third reduced data items have a frequency of occurrence greater than a specified amount, however it would have been obvious for one of ordinary skill in the art to modify the invention disclosed by Cox into the claimed invention due to disclosure of "the routing device [storing] information about the attack for later use and for analysis for administrators of the private network. For example, information concerning the packet origination, destination or content can be stored internally to the router device or sent to a syslog server for later analysis." The motivation here would be that such data stored for analysis and used as claimed would allow the administrators to act more proactively and better filter out data which have potential of causing network attacks (col. 4 lines 9-14).

Further Townshend does disclose determining frequently occurring sections in column 2 lines 11-14. It would have been obvious to combine these two inventions and the motivation would be to improve how proactively the invention behaves and allow for better filtering of data which have potential of causing network attacks

Regarding claim 10, Cox et al., is silent in disclosing a collection of data items comprises a portion of the network payload, however Towshend does disclose network payload and the signatures disclosed in Townshend are the models used in predicting possible threats to the network, which by definition are what network payloads are. The motivation for the combination is to provide better means of determining the threat level of data being analyzed.

Regarding claim 16, Cox et al., discloses a method as in claim 10, wherein said collection of data items further comprises a portion of a network header (Rejected under the same rationale as claim 10).

Regarding claim 17, Cox et al., discloses a method as in claim 11, wherein said portion of a network header comprises a port number indicating a service requested by a network packet (Rejected under the same rationale as claim 7).

Regarding claim 18, Cox et al., discloses a method as in claim 17, wherein said port number comprises a source port or a destination port (Rejected under the same rationale as claim 7).

Regarding claim 19, Cox et al., discloses a method as in claim 1, wherein said data items comprise a first subset of a network packet including payload and header; and the method further comprises obtaining a second subset of the same network packet for subsequent analysis (Rejected under the same rationale as claim 10).

Regarding claim 22, Cox et al., discloses a method as in claim 2, wherein said reducing said data items and said determining frequently occurring sections comprises: taking a first hash function of said data items first maintaining a first counter, with a plurality of stages, and incrementing one of said stages based on an output of said first hash function; taking a second hash function of said data items; and second maintaining a second counter, with a plurality of stages, and incrementing one of said stages of said second counter based on an output of said second hash function (Rejected under the combined rationales as claim 8).

Regarding claim 23, Cox et al., discloses a method as in claim 22, further comprising checking said one of said stages of said first counter and said one of said stages of said second counter against a threshold, and identifying a first reduced data item as associated with frequently occuring content only when both said one of said stages of said first counter and said one of said stages of said second counter are both above said threshold (Rejected under the same rationale as claim 11).

Regarding claim 24, Cox et al., discloses a method as in claim 23, further comprising adding

the first reduced data item to a frequent content buffer table (Rejected under the same rationale as claim 11).

Regarding claim 25, Cox et al., discloses a method as in claim 24, further comprising taking at least a third hash function of said data items, and incrementing a stage of at least a third counter based on said third hash function, where said identifying said first reduced data item as associated with frequently occurring content only when all of said stages of each of said first, second and third counters are each above said threshold (Rejected under the same rationale as claim 8).

Regarding claim 26, Cox et al., discloses a method as in claim 22, further comprising obtaining said data items by taking a first part of messages, and subsequently obtaining a new data items by taking a second part of the messages (Rejected under the same rationale as claim 1).

Regarding claim 27, Cox et al., discloses a method as in claim 26, wherein at least one of said hash functions comprises an incremental hash function (Rejected under the same rationale as claim 8).

Regarding claim 28, Cox et al., discloses a method as in claim 3, wherein reducing said data items comprise hashing at least one of the source or destination, to form a collection of hash values, first determining a unique number of said hash values, and second determining a

number of said one of source or destination addresses based on said first determining (Rejected under the same rationale as claim 8).

Regarding claim 29, Cox et al., discloses a method as in claim 28, further comprising scaling the hash values prior to said second determining (Rejected under the same rationale as claim 8).

Regarding claim 30, Cox et al., discloses a method as in claim 29, wherein said scaling comprises scaling by a first value during a first counting session, and scaling by a second value during a second measurement session (Rejected under the same rationale as claim 8).

Regarding claim 31, Cox et al., discloses a method as in claim 7, wherein said detecting code comprises looking for a first valid opcode at a first location, based on said first valid opcode, determining a second location representing an offset to said first valid opcode, and looking for a second valid opcode at said second location (Rejected under the same rationale as claim 7).

Regarding claim 32, Cox et al., discloses a method as in claim 31, further comprising establishing that a first section includes code when a predetermined number of valid opcodes are found at proper distances (Rejected under the same rationale as claim 7).

Regarding claim 70, Cox et al., discloses a method as in claim 69, wherein said monitoring network content comprises obtaining both portions of the data on the network, and

portnumbers indicating a services requested by network packets (Rejected under the same rationale as claims 17 and 18).

Regarding claim 72, Cox et al., discloses a method as in claim 71, wherein said data reduction function comprises a hash function (Rejected under the same rationale as claim 8).

Regarding claim 73, Cox et al., discloses a method as in claim 72, wherein said data reduction function comprises an incremental hash function Rejected under the same rationale as claim 8).

Regarding claim 74, Cox et al., discloses a method as in claim 69, wherein data reducing said portions comprises using said data reduction function in a scalable configuration (Rejected under the same rationale as claim 8).

Regarding claim 76, Cox et al., discloses a method as in claim 75, wherein said second data reducing comprises hashing said address information (Rejected under the same rationale as claim 8).

Regarding claim 77, Cox et al., discloses a method as in claim 69, further comprising testing contents of the frequent content to determine the presence of code in said frequent content (Rejected under the same rationale as claim 7).

Regarding claim 78, Cox et al., discloses a method as in claim 77, wherein said testing contents comprises identifying an opcode in said frequent content, determining a length of the opcode, and looking for another opcode at a location within said frequent content based on said length Rejected under the same rationale as claim 7).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHINWENDU C. OKORONKWO whose telephone number is (571)272-2662. The examiner can normally be reached on MWF 2:30 - 6:00, TR 9:00-3:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Chinwendu C Okoronkwo/
Examiner, Art Unit 2136

May 15, 2008

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136